

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

RYAN HIGGS and ALYSSA WOJNAR
on behalf of themselves and all others
similarly situated,
Plaintiffs,

v.

OAKBEND MEDICAL CENTER,
Defendant.

§
§
§
§
§
§
§
§
§
§

CASE NO. 4:22-cv-07340

CLASS ACTION COMPLAINT

Plaintiffs Ryan Higgs and Alyssa Wojnar (“Plaintiffs”), individually and on behalf of all others similarly situated (“Class Members”), bring this Class Action Petition against Defendant OakBend Medical Center (hereinafter “OakBend” or “Defendant”), a Texas corporation. Plaintiffs seek damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack against Defendant that allowed a third party to access Defendant’s computer systems and data, resulting in the compromise of highly sensitive personal information (the “Data Breach”). Because of the Data Breach, Plaintiffs and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their sensitive personal information.

2. Upon information and believe, the information compromised in the Data Breach is

confidential personally identifiable information and personal health information of Defendant's current and former patients (collectively the "Private Information").

3. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party or precisely what specific type of information was accessed.

4. On information and belief, Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to a cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

5. In addition, on information and belief, Defendant failed to properly monitor the computer network and IT systems that contained the Private Information.

6. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct—since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *inter alia*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing

fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now—and in the future—closely monitor their financial accounts to guard against identity theft.

9. Plaintiffs and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

11. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

12. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (1) negligence, (2) breach of implied contract; (3) negligence per se; (4) breach of fiduciary duty; (5) intrusion upon seclusion/invasion of privacy and (6) unjust enrichment.

PARTIES

13. Plaintiff Alyssa Wojnar (formerly Casey) is a natural person and a citizen of the State of Pennsylvania. She resides in Pendel, Pennsylvania and has no intention of moving to a

different state in the immediate future

14. Plaintiff Ryan Higgs is a natural person and a citizen of the State of Illinois. He resides in Chicago, Illinois and has no intention of moving to a different state in the immediate future.

15. Defendant is a Texas corporation with a registered office in Fort Bend County—at 1705 Jackson St., Richmond, Texas 77469.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2), because this is a class action involving more than one hundred putative class members and the amount in controversy exceeds \$5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiffs (and many members of the class) are citizens of states different than Defendant's.

17. This Court has general personal jurisdiction over Defendant because Defendant principal place of business and headquarters are in Texas. And moreover, Defendant regularly conducts substantial business in Texas.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

Defendant Collected and Stored the Private Information of Plaintiffs and Class Members

19. Defendant is a medical service provider in the Greater Houston Area.¹ It has over

¹ *Facts*, OAKBEND MEDICAL CENTER, <https://www.oakbendmedcenter.org/facts/> (last visited Oct. 25, 2022).

1,200 employees and fifty locations.² Each year, Defendant receives 8,500 inpatients visits, 40,000 emergency room visits, and 100,000 outpatient visits.³

20. In the ordinary course of business, Defendant's patients must provide—as Plaintiffs did here—their Private Information to receive Defendant's services.

21. Defendant agreed to and undertook legal duties to maintain the Private Information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws.

22. Defendant held the Private Information of Plaintiffs and Class Members.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

24. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. And Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, and to make only authorized disclosures of this information.

Defendant's Data Breach

25. Defendant failed in its duties on September 1, 2022, when its inadequate security practices resulted in the Data Breach.⁴ Defendant was overwhelmed by a ransomware attack—where criminals access sensitive files, encrypt those files, and then demand ransom payment for

² *Id.*

³ *Id.*

⁴ *Important Announcement, OAKBEND MEDICAL CENTER*, <https://www.oakbendmedcenter.org/> (last accessed Oct. 25, 2022).

the decryption key.⁵ Over a month later, on October 11, 2022, Defendant admitted that “some of our patients and community members are receiving emails sent by third parties regarding the recent ransomware attack.”⁶

26. A cybercriminal group has taken credit for the Data Breach of Defendant’s network.⁷ Specifically, the group “Daixin Team” claims to have caused the breach—and then stole over one million patient records.⁸

27. Daixin Team claims to have stolen names, dates of birth, patient treatment information, and Social Security Numbers.⁹ Now, the group warns that it will release a “full leak” of the stolen data.¹⁰

28. Daixin Team is a particularly infamous and dangerous cybercriminal group. For one, it was responsible for a data breach of a Missouri-based hospital.¹¹ There, Daixin Team accessed and stole names, dates of birth, medical record numbers, patient account numbers, Social Security numbers, and medical and treatment information.¹² Then, the Daixin Team published the stolen Private Information on the Dark Web.¹³

29. And recently, an official “Cybersecurity Advisory” on Daixin Team was released

⁵ *Id.*

⁶ *Id.*

⁷ Naomi Diaz, *Ransomware Group Threatens to Leak 1M Patient Records from Texas Hospital*, BECKER’S HEALTH IT (Sept. 14, 2022) <https://www.beckershospitalreview.com/cybersecurity/ransomware-group-threatens-to-leak-1m-patient-records-from-texas-hospital.html>.

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Fitzgibbon Hospital, Diskriter, Christiana Spine Center Suffer Ransomware Attacks*, HIPAA JOURNAL (June 29, 2022) <https://www.hipaajournal.com/fitzgibbon-hospital-diskriter-christiana-spine-center-suffer-ransomware-attacks/>.

¹² *Id.*

¹³ *Id.*

by the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Department of Health and Human Services (HHS).¹⁴

30. This official advisory warns that Daixin Team targets the healthcare sector.¹⁵ And so far, Daixin Team has successfully “[e]xfiltrated personal identifiable information (PII) and patient health information (PHI) and threatened to release the information if a ransom is not paid.”¹⁶

31. In terms of tactics, the official advisory reveals that Daixin Team has “[d]eployed ransomware to encrypt servers responsible for healthcare services—including electronic health records services, diagnostics services, imaging services, and intranet services.”¹⁷

32. And here, the Daixin Team has already publicly leaked some of the data stolen in Defendant’s Data Breach.¹⁸

33. Thus, upon information and belief, the Data Breach was the result of a deliberate attempt by criminals to access to Private Information of Plaintiffs and the Class Members.

34. And upon information and belief, more than one million individuals had their Private Information exposed in the Data Breach. Also, upon information and belief, the Private Information exposed was not encrypted.

35. Defendant had obligations created by contract law, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

¹⁴ *Joint Cybersecurity Advisory*, FEDERAL BUREAU OF INVESTIGATION (Oct. 21, 2022) <https://www.ic3.gov/Media/News/2022/221021.pdf>.

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *OakBend Medical Center Suffers Ransomware Attack*, HIPAA JOURNAL (Sept. 13, 2022) <https://www.hipaajournal.com/oakbend-medical-center-suffers-ransomware-attack/>.

36. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

37. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.¹⁹ Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.²⁰ The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.²¹

38. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."²²

39. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.²³

40. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

¹⁹ See *2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) <https://notified.idtheftcenter.org/s/>.

²⁰ *Id.*

²¹ *Id.*

²² Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

²³ See Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack> (last visited July 31, 2022).

Defendant Fails to Comply with FTC Guidelines

41. The Federal Trade Commission (“FTC”) promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

42. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.²⁴ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²⁵

43. The FTC further recommends that companies not maintain personally identifiable information (“PII”) longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

44. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate

²⁴ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

²⁵ *Id.*

measures to protect against unauthorized access to confidential Consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

45. Defendant failed to properly implement basic data security practices.

46. Defendant was at all times fully aware of its obligation to protect the Private Information of persons who had provided it to Defendant, including its patients and all other individuals whose personal information it maintained. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

47. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

48. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

49. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

50. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant Violated HIPAA

51. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.²⁶

52. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.²⁷

53. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. §

²⁶ HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

²⁷ See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

164.306(a)(1);

- b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);
- e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R.

§ 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

- i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

54. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant's Negligence

55. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches;
- b. Failing to adequately protect patients Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to train its employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to maintain adequate email security practices;
- e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;
- f. Failing to comply with FTC guidelines for cybersecurity, in violation of

Section 5 of the FTC Act; and

g. Failing to adhere to industry standards for cybersecurity.

56. As the result of antivirus and malware protection software in dire need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Defendant's IT systems and remove data which contained unsecured and unencrypted Private Information.

57. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant.

Data Breaches Cause Disruption and Put Persons at an Increased Risk of Fraud and Identity Theft

58. Data breaches are problematic because the breaches can negatively impact the overall daily lives of individuals affected by the attack.

59. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."²⁸

60. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, taking over victims' identities

²⁸ See GAO-07-737: *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV. ACCOUNTING OFFICE (2007) <https://www.gao.gov/new.items/d07737.pdf>.

in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

61. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁹

62. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

63. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give

²⁹ See *IdentityTheft.gov*, FEDERAL TRADE COMMISSION, <https://www.identitytheft.gov/Steps> (last visited July 31, 2022).

the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

64. Moreover, theft of Private Information results in the loss of a valuable property right.³⁰

65. Notably, there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and between when Private Information and/or financial information is stolen and when it is used.

66. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

67. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

68. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

69. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and

³⁰ *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

medical accounts for many years to come.

70. Sensitive Private Information can sell for as much as \$363 per record according to the Infosec Institute.³¹ Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

71. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.³² Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.³³ Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

72. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

73. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security

³¹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited July 31, 2022).

³² *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION (2018) www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 31, 2022).

³³ *Id.* at 4.

number.”

74. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”

75. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just \$1 in 2016 – the same as a Facebook account.³⁴ That pales in comparison with the asking price for medical data, which was selling for \$50 and up.³⁵

76. Because of the value of its collected and stored data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

77. For this reason, Defendant knew or should have known about these dangers and strengthened its data security accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

The Experiences—and Injuries—of Plaintiffs and Class Members

78. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant has merely offered Plaintiffs and Class Members 18 months of free credit monitoring. But this does not to compensate them for damages incurred and time spent dealing with the Data Breach. Signing up

³⁴ See Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LOGDOG (Feb. 14, 2016), <https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/>.

³⁵ Lisa Vaas, *Cyberattacks Paralyze, and Sometimes Crush, Hospitals*, NAKED SECURITY (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/> (last visited July 1, 2022);

for this service requires Plaintiffs and Class Members to forfeit time that could otherwise be spent making money or enjoying life.

79. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

80. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

81. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

82. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

83. Plaintiffs and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to (i) damage to and diminution in the value of their Private Information, a form of property that Defendant obtained from Plaintiffs and Class Members; (ii) violation of their privacy rights; and (iii) imminent and impending injury arising from the increased risk of identity theft and fraud; and (iv) emotional distress.

84. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct

result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing “freezes” and “alerts” with reporting agencies;
- d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- e. Contacting financial institutions and closing or modifying financial accounts; and
- f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

85. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

Plaintiff Higgs’ Experience

86. Plaintiff Higgs is a former patient of Defendant. He last used their services in 2018.

87. Thus far, Plaintiff Higgs has not received any notice or warning from Defendant. And yet, Plaintiff Higgs' Personal Information was certainly exposed in the Data Breach.

88. For one, Plaintiff Higgs was notified by Chase Bank that his personally identifying information, including his Social Security Number, were found on the dark web related to the OakBend breach.

89. Numerous identity protection services have reaffirmed that Plaintiff Higgs' Personal Information was exposed in the Data Breach. For example, he received an "Identity Risk" alert warning him that "[y]our Social Security number has been leaked." And that alert revealed that the source of the leak was "oakbendmedcenter.org."

90. Plaintiff Higgs also received an alert stating, "Compromised Information Found." Specifically, that alert warned that "[w]e found your Social Security Number on the Dark Web." Again, this alert revealed that the source of the leak was "oakbendmedcenter.org."

91. And since the breach, Plaintiff has started receiving spam texts or spam phone calls.

92. Even worse, Plaintiff has received numerous requests about Section 8 assistance, food assistance, and finishing loan applications, all of which are fraudulent.

93. In short, it appears that his personal information is being used for a litany of fraudulent assistance applications and purchases.

94. As a condition of receiving services through OakBend, Plaintiff Higgs entrusted confidential information such as his name, address, date of birth, Social Security number and other personally identifiable information to Defendant with the reasonable expectation and understanding that Defendant would take, at a minimum, industry standard precautions to protect,

maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to him.

95. As a result of the Data Breach, Plaintiff Higgs made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

96. Plaintiff Higgs suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (i) damage to and diminution in the value of his Private Information—a form of property that Defendant obtained from Plaintiff; (ii) violation of his privacy rights; (iii) the likely theft of his Private Information and (iv) imminent and impending injury arising from the increased risk of identity theft and fraud.

97. As a result of the Data Breach, Plaintiff Higgs also suffered emotional distress because of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Higgs is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

98. As a result of the Data Breach, Plaintiff Higgs anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Higgs will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

Plaintiff Wojnar's Experience

99. Plaintiff Wojnar is a former patient of Defendant. Specifically, she used its medical services once in approximately December 2021 in Sugarland, Texas.

100. Thus far, Plaintiff Wojnar has not received any notice or warning from Defendant. And yet, Plaintiff Wojnar's Personal Information was certainly exposed in the Data Breach.

101. For one, Plaintiff Wojnar was notified that her Private Information was published on the Dark Web. Specifically, Experian informed her that her SSN was found on the Dark Web—stemming from the OakBend Data Breach.

102. Since the breach, she purchased additional protection services from Experian—for approximately \$23 per month.

103. And since the breach, Plaintiff has started receiving spam texts or spam phone calls.

104. As a condition of receiving services, Plaintiff Wojnar entrusted confidential information such as her name, address, date of birth, Social Security number and other personally identifiable information to Defendant with the reasonable expectation and understanding that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to him.

105. As a result of the Data Breach, Plaintiff Wojnar made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

106. Plaintiff Wojnar suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (i) damage to and diminution in the value of her Private Information—a form of property that Defendant obtained from Plaintiff; (ii) violation of her privacy rights; (iii) the likely theft of her Private Information

and (iv) imminent and impending injury arising from the increased risk of identity theft and fraud.

107. As a result of the Data Breach, Plaintiff Wojnar also suffered emotional distress because of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using their Private Information for purposes of identity theft and fraud. Plaintiff is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

108. As a result of the Data Breach, Plaintiff Wojnar anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

CLASS ACTION ALLEGATIONS

109. Plaintiffs bring this action on behalf of themselves and all other persons similarly situated.

110. Plaintiffs proposes the following Class definition, subject to amendment as appropriate:

All persons residing in the United States whose information was compromised by the Data Breach—including all persons that Defendant sent a notice of the Data Breach to (the “Nationwide Class”).

111. Plaintiffs also propose the following subclass, to be represented by Plaintiff Higgs:

All persons residing in Illinois whose information was compromised by the Data Breach—including all persons that Defendant sent a notice of the Data Breach to (the “Illinois Subclass”).

Together, the Nationwide Class and the Illinois Subclass are referred to as the “Class.”

112. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

113. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification.

114. Numerosity. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of the approximately one million patients whose Private Information was compromised in the Data Breach.

115. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiffs and Class Members suffered legally cognizable damages because of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant's conduct was per se negligent;
- l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- m. Whether Defendant was unjustly enriched;
- n. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- o. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

116. Typicality. Plaintiffs' claims are typical of those of other Class Members

because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach.

117. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

118. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

119. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

120. Defendant has acted on grounds that apply generally to the Class as a whole, so

that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

121. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely notify the public of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard patient Private Information; and
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

122. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class

Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and All Class Members)

123. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

124. Defendant required Plaintiffs and Class Members to submit non-public personal information in order to obtain healthcare services, which they then stored and maintained in its computer networks.

125. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duties included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

126. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

127. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant were

in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

128. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

129. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

130. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

131. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failure to periodically ensure that its email system had plans in place to

maintain reasonable data security safeguards;

- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

132. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

133. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

134. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

135. Defendant's negligent conduct is ongoing, in that they still hold the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

136. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

137. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

138. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

139. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

140. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

141. Plaintiffs and Class Members paid money to Defendant or provided their Private Information to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

142. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

143. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

144. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

145. Defendant breached its implied contracts with Class Members by failing to

safeguard and protect their Private Information.

146. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

147. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

148. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CAUSE OF ACTION
Negligence Per Se
(On Behalf of Plaintiffs and All Class Members)

149. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

150. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

151. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiffs and Class Members' Private Information.

152. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

153. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

154. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

155. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

156. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

157. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and All Class Members)

158. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

159. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs and Class Members' Private Information, Defendant became fiduciaries by its undertaking and guardianship of the Private

Information, to act primarily for Plaintiffs and Class Members, (i) for the safeguarding of Plaintiffs and Class Members' Private Information; (ii) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (iii) to maintain complete and accurate records of what information (and where) Defendant did and do store.

160. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationships with its patients, in particular, to keep secure its patients' Private Information.

161. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

162. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs and Class Members' Private Information.

163. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

164. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

165. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual

and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

166. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
Intrusion Upon Seclusion/Invasion of Privacy
(On Behalf of Plaintiffs and All Class Members)

167. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

168. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

169. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

170. Defendant's conduct as alleged above intruded upon Plaintiffs' and Class

Members' seclusion under common law.

171. By intentionally failing to keep Plaintiffs' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs and Class Members' privacy by:

- a. Intentionally and substantially intruding into Plaintiffs and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person;
- b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and
- c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

172. Defendant knew that an ordinary person in Plaintiffs' or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

173. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

174. Defendant intentionally concealed from and delayed reporting to Plaintiffs and Class Members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

175. The conduct described above was at or directed at Plaintiffs and the Class Members.

176. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that

an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

177. In failing to protect Plaintiffs' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class.

SIXTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and All Class Members)

178. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

179. Plaintiffs bring this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of implied contract count.

180. Upon information and belief, Defendant fund its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members or revenue derived from the use of their Private Information.

181. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members or derived from their Private Information is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

182. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and/or services from Defendant and/or its agents and provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have

their Private Information protected with adequate data security.

183. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

184. In particular, Defendant enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

185. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

186. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

187. Defendant acquired the Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

188. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

189. Plaintiffs and Class Members have no adequate remedy at law.

190. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

191. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

192. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

SEVENTH CAUSE OF ACTION
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"),
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(On behalf of Plaintiff Higgs and the Illinois Subclass)

193. Plaintiff Higgs re-alleges and incorporate by reference all other paragraphs in the

Complaint as if fully set forth herein.

194. Plaintiff Higgs and the Illinois Subclass are “consumers” as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff Higgs, the Illinois Subclass, and Defendant are “persons” as defined in 815 Ill. Comp. Stat. § 505/1(c).

195. Defendant engaged in “trade” or “commerce,” including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of “merchandise” (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

196. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of its services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiff’s and the Illinois Subclass Members’ sensitive Private Information from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act and HIPAA; (ii) failing to disclose or omitting materials facts to Plaintiff and the Illinois Subclass regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the Private Information of Plaintiff and the Illinois Subclass; (iii) failing to disclose or omitting materials facts to Plaintiff and the Illinois Subclass about Defendant’s failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Private Information of Plaintiff and the Illinois Subclass; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff’s and the Illinois Subclass’s Private Information from further unauthorized disclosure, release, data breaches, and theft.

197. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable

state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Illinois Subclass and defeat their reasonable expectations about the security of their Private Information.

198. Defendant intended that Plaintiff and the Illinois Subclass rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

199. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Illinois Subclass. Plaintiff and the Illinois Subclass have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

200. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Illinois Subclass of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*

201. As a result of Defendant's wrongful conduct, Plaintiff and the Illinois Subclass were injured in that they never would have provided their Private Information to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their Private Information from being hacked and taken and misused by others.

202. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff and the Illinois Subclass have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost

opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Illinois Subclass Members.

203. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff Higgs and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

- D. For an award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for any and all issues in this action so triable as of right.

Dated: October 28, 2022

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
SDTX Bar No. 30973
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Samuel J. Strauss*
Raina C. Borrelli*
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com

ATTORNEYS FOR PLAINTIFFS

***Pro Hac Vice Forthcoming**